Number 2-97

# security awareness bulletin



*Inside*

**Empowering the Security Professional**



*plus more*



Department of Defense Security Institute, Richmond, Virginia

# security awareness bulletin

Approved for open publication — Unlimited reproduction authorized

June 1997

**Director**
**Department of Defense Security Institute**
R. Everett Gravelle

**Editor**
Lynn Fischer

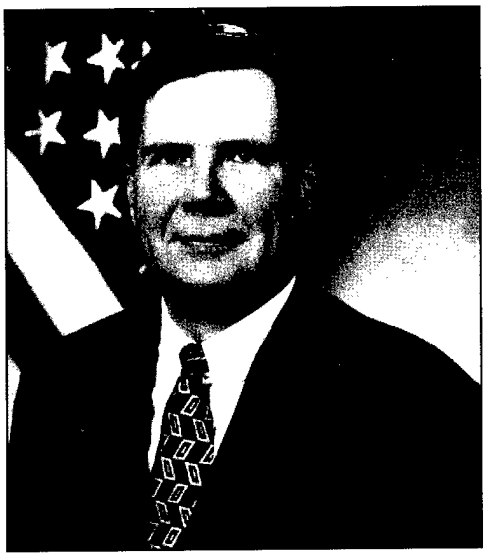
The Security Awareness Bulletin is produced by the Department of Defense Security Institute, Richmond, Virginia. Our purpose is to promote security awareness and compliance with security procedures through dissemination of information to security trainers regarding current security and counterintelligence developments, training aids, and education methods.

**For new distribution or address changes:**

- Air Force: Contact your local Publication Distribution Office. Ask for "DODSISAB."
- Army, Navy, Marine Corps, and Department of Defense agencies: DoD Security Institute, Attn: SEAT, 8000 Jefferson Davis Hwy, Richmond, VA 23297-5091, POC Tracy Gulledge, (804) 279-4223, DSN 695-4223; fax (804) 279-6406, DSN 695-6406. E-Mail gulledget@dodsi.dscr.dla.mil
- For other government agencies and contractors, you can order this publication through the Government Printing Office (see page 35), or download it from the Internet. Our URL is http://www.dtic.mil/dodsi

INTRODUCING

## Mr. J. William Leonard
## Director, Security Programs
## Office of the Secretary of Defense



I am delighted to be afforded this opportunity to share some thoughts with my fellow security practitioners within the Department of Defense, its contractors, and other organizations within the Federal Government. As a community, we have achieved many accomplishments. I am confident that we are well poised to accept the challenges of the 21st century.

Today our society is well underway in its transition from the Industrial to the Information Age. In the U.S., over 60 percent of the workforce is engaged in information-related activities. The value of most wealth producing-resources depends on "knowledge capital" and not on financial assets or masses of labor. Similarly, the doctrine of the U.S. military is now principally based on the superior use of information. Such a monumental transition poses significant challenges for the security community.

First, it is incumbent upon us today to be developing strategies by which to facilitate the dissemination and sharing of information – albeit securely, not only with the operators in the field, but with foreign partners in either a coalition military operation or in the development and production of state-of-the-art weapons systems.

Secondly, in the Information Age, we need to become more adept at security which emphasizes the reliable performance of the massive information systems and networks that control the basic functions of our infrastructure. Protecting the confidentiality, integrity, and availability of the nation's information systems and information assets – both public and private – has replaced the traditional response of achieving security by locking information in an inaccessible container.

Thirdly, we also need to remain mindful of security costs. We must ensure that the sizable costs of information security – to include the tangible costs of needlessly guarding certain information and the intangible costs of depriving ourselves of the fullest flow of information – do not divert scarce resources that can be better directed to modernization and other readiness issues.

Whereas the technological advancements of the Information Age will be the source of many security challenges for years to come, it will also be a source for many solutions. It is incumbent upon all security practitioners to not only become conversant with the technology, but to achieve connectivity to the Internet. As with many other disciplines, the Web will be the primary means for the delivery of security awareness and educational materials and publications as well as other information essential to the proficiency of the security professional.

I am looking forward to collectively working with all of you in ensuring that the security community remains relevant in the achievement of the Department of Defense's overall goals and objectives.

*It is incumbent upon all security practitioners to not only become conversant with the technology, but to achieve connectivity to the Internet.*

# J. William Leonard

Bill Leonard, a native of New York City, was appointed to serve as the Director, Security Programs in the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) in December 1996. He is responsible for the development and oversight of security policy and procedures for classification management, personnel, industrial, physical, nuclear, port, overflight and operational security, as well as security countermeasures education and training. In addition to serving as the executive agent for the National Industrial Security Program, he also guides and directs the Acquisition Systems Protection Program and the Defense Treaty Inspection Readiness Program.

Prior to his current assignment, Mr. Leonard served as the Director, Planning and Inspections at the Defense Investigative Service (DIS). He was also an Assistant Deputy Director (Industrial Security) for DIS from 1992-1996 and from 1985-1989. In that capacity, he was responsible for a wide range of policy and operational matters pertaining to the DoD's administration of the National Industrial Security Program (NISP), both within the U.S. and overseas. He was also instrumental in the establishment of the DIS Counterintelligence Office.

From 1989-1992, Mr. Leonard served as the Director, Office of Industrial Security International in Brussels, Belgium. Previous assignments included additional tours at Headquarters, DIS, as well as serving as an instructor at the Defense Industrial Security Institute in Richmond, Virginia. He was also a Command Security Officer at a DoD activity, as well as an Industrial Security Representative in the New York City area. He joined the federal service in 1973.

Mr. Leonard holds a Bachelor of Arts degree in History from St. John's University in New York City and a Master of Arts degree in International Relations from Boston University. Noteworthy awards which Mr. Leonard has received include the DIS Exceptional Service Award (1987) as well as the DIS Meritorious Service Award (1989 and 1993). He currently resides in southern Maryland with his wife, Clarice. They have three children, John, Michael, and Jessica.

# Intranet For Security Professionals

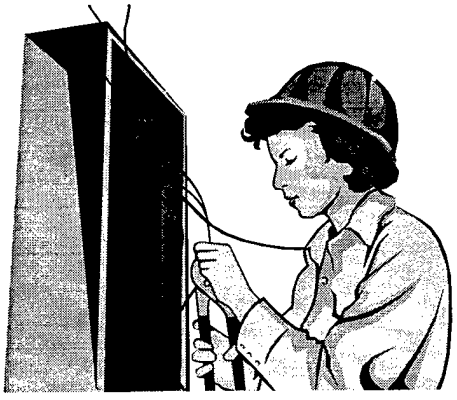
## CONSTRUCTION ZONE

BY LYNN F. FISCHER, DOD SECURITY INSTITUTE

To quote the great and prophetic Yogi Berra, "The future ain't what it used to be." And what follows is another superb example of that altered vision of what is to come—as if technology wasn't already moving fast enough to make our heads spin:

### The Dawn of Private Networks

The technologies which made it possible for us to enjoy e-mail communication through the Internet and the mushrooming World-Wide Web, have also made it possible to set up "private" networks for members of a firm, organization, or communities of professionals having common interests and who desire a degree of confidentiality in their information exchange. These private networks are called INTRANETS as opposed to *the* INTERNET which is accessible to all the world. However, to get into an intranet as a legitimate user, one must go through the Internet, addressing the private network with a URL (Universal Resource Locator) address.



The use of professional intranets offers many opportunities to share sensitive information in radical new ways, and very affordably. Intranets break down the stove pipe databases that currently impede timely administrative responses. Because the intranet software is open based, non-platform specific, it makes use of existing investments in computers, servers, mainframes, databases, applications, and networks. This means that a new intranet, at little or no additional cost, can absorb an existing infrastructure. Commercial companies that have used intranets for linking their business elements together are claiming a 1500% return on investment.

Just as on the Internet, an intranet can support a web site, but the site would be available only to those who have authorized access to that private network.

### The ISP Initiative

Here's where the security community comes in. Like any widely dispersed group of people with common interests and needs, security professionals in government and industry would benefit considerably from their own intranet. We need to share information and ideas, we are scattered all over the globe, and with minimal investment in hardware or software, we might take advantage of this new technology.

For this reason, the Defense Advanced Research Projects Agency (DARPA) has undertaken a 12-month study to determine what it will take to design a private network for security professionals

and get it up and running. Under the direction of DARPA's Matt Donlon, working out of the Department of Defense Security Institute, participants from several federal government and industry security activities are working together to explore the feasibility, identify any barriers, estimate costs and the level of security, specify the architecture, and identify the potential users and data providers.

It should be pointed out that the Defense Advanced Research Project Agency has a unique track record in network development. It was this agency that, in developing the ARPAnet in the late 1960s, laid the foundation for the Internet. ARPAnet soon evolved to the MILNET in the 1970s and then the Internet in the '90s as the user base broadened to include the private sector. DARPA could in fact be credited with inventing the Internet. The original ARPAnet was designed as a military communications wide-area network. Its mission was to provide connectivity among university-based researchers that would allow survivability during a nuclear war.

## The ISP Prototype: Here and now

The new ***Intranet for the Security Professional*** **(ISP)** will exploit wide-area network technologies to radically change the security community's way of doing business. The first step in this process is to test a prototype, a "virtual private network," that is already up and running. Its primary function is to collect data, ideas, and comments from potential users and contributors. If you have access to the Internet World Wide Web we invite you to take a look at the prototype and sign up as an ISP Member. You will find it at:

***http://isp.hpc.org***

There is a deliberate effort here to make ISP development a collective effort and to set up functions which mirror demands and needs in the community. The Simulated Prototype also serves as a vehicle for input on security policy development (currently, the National Industrial Security Program Operating Manual (NISPOM) Chapter 8 re-write) and it allows users to download several articles about the explosion of intranets in government and the private sector.

## Are we ready for this?

This is a fair question: Do our professionals in the field right now have the hardware and software to get on line? A recent survey of security facilities in government and industry indicates that most have what it takes. 70% have Internet access, 75% use interoffice e-mail, and 70% of business personnel are already "browsing the web."


The potential users are there. In addition there are some real problems in the security community that are not going to go away without a significant change in the way we do business. Here are some of the frequently heard complaints: Mounting security costs for government programs are the regular subject of media exposés and Congressional commissions. Policy development time is excessive, and once promulgated, its implementation lacks uniformity. The passing and verification of clearances is a time-consuming and complicated business. Essential information about policy changes, the threat, alerts and high-risk situations,

training opportunities, and just plain policy guidance doesn't trickle down to the workers in the field. In summary there are communication blockages, stovepipes, and constrictions that must be eliminated before we can do our work effectively.

As stated on its opening web page, ISP is an initiative to provide a very affordable, trusted, real-time communication infrastructure to meet the objectives of Presidential Decision Directive (PDD) #29 (1994). PDD 29 challenges the security community (in this do-more-with-less era) to write security policies and procedures that are flexible enough to change as the threat evolves; to be consistently efficient in the allocation of scarce resources; and to provide the security we need at the price we can afford. In a realistic sense, past methods of meeting these objectives have failed. The missing link is an enabling tool to facilitate information exchange. The ISP concept was conceived to be that enabling technology for answering the challenge of PDD 29 and to address the many problems with security today cited by security professionals and concerned citizens.

## What the ISP might do for us in the future

While it is clear that its ultimate features will reflect what the users say they need, several objectives have been identified as desirable capabilities: 1) input and debate related to security policy development, 2) dissemination of current threat information, 3) on-line clearance verification, and 4) information about educational products and security events. Through its supporter registration feature, the prototype is bringing on-line a pool of industry and government participants that will come up with many new ideas and help shape the ISP for further development. Drawing on the inventory of proposals and expressed concerns, ISP planners are developing a concept of operations as well as an ISP security policy for data providers and end users.

By using Intranet technologies, the ISP will remove the traditional time and space boundaries that now exist in the world of the security professional. This will be accomplished by providing the security community the one-stop shopping for critical information, offering virtual meeting rooms for fast exchange of information, collaborative document building tools to speed policy development, the automation of tasks now carried out via fax and phone, and critical information messaging services.

Ultimately, the ISP could bring the security community (both government and industry) on-line together in a trusted link. The community would have on-line access to threat information, classification guides, declassification guidelines & coordination, education and training support, supply and equipment tools, a security professionals' email directory, links to all security offices, clearance verifications & visit certifications, a security reference library, standard forms, live connectivity to the Defense Investigative Service, and much more.

Another future component of ISP, separate from the "private" or protected enclave, will be the introduction of connectivity to the public, which will enable interface and information sharing to interested players outside of the security community. This concept allows for a better understanding of our place in the big picture of government services and will support initiatives relating to access to the government by the general public.

## Looking forward to the 21st century

The ISP vision for the security profession in the next millennium is to build the affordable infrastructure that will lead to a paperless workplace, have web-based access to all databases, reduce cost, be responsive to post-cold war risk management philosophies, leap frog today's problems with technology solutions, have means to access the public, and create a real time information flow.

The ***Intranet for Security Professionals*** is a tool for the infusion of technology into the business process. The ISP will provide the nation a better security service by modernizing the security management practices, reducing the cost of doing business, and increasing the credibility of the security profession.

**Shoot us your ideas for ISP features and capabilities. No idea will be rejected as too wild or ambitious. Sign on as an ISP supporter today.** [***http://isp.hpc.org***]

## Downlink DoDSI presents the

# *"Information Security Management Course"*

*via video teletraining*

The Information Security Team of the Department of Defense Security Institute (DoDSI) will broadcast the Information Security Management Course (ISMC) to classrooms across the United States on the following dates:

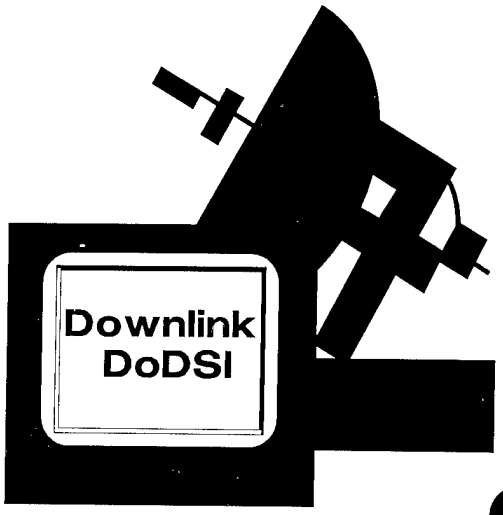
| | |
|---|---|
| **16 - 25 September** | **(East Coast and Central Time Zones)** |
| **02 - 11 December** | **(Mountain and Pacific Time Zones)** |

If your installation can receive a satellite training broadcast (and it probably can), then you may want to subscribe to this training opportunity. Video teletraining is a highly cost-effective alternative to on-site, instructor-led training. If your training budget requires creative alternatives, video teletraining may be the solution. This training will be presented ***at no charge*** to the receiving activity.

The ISMC provides a comprehensive discussion of the DoD Information Security Program, to include the proper classification, downgrading and declassification of information, and safeguarding of classified information against unauthorized disclosure. Students will have the opportunity to discuss ideas, issues, problems and possible solutions with information security professionals. The course is designed for DoD military personnel and civilians with primary duty as a security manager within a DoD component information security program.

This resident course has been reengineered to be presented via interactive video teletraining. The course will be conducted over the Satellite Education Network (SEN) from its studios at Fort Lee, Virginia. Most military installations have the capability to take part in video teletraining. The SEN, 3.3 compressed digital system, is compatible with the Air Force Training Network, T-Net, and Warrior, and can be bridged to the Navy's C-Net.

The receiving site will have to provide an information security subject matter expert to help facilitate the course. The facilitator should have previously completed the resident ISMC and be available during course hours to assist the DoDSI faculty in conducting the course. The facilitator will be responsible for leading off-line activities such as practical exercises, quizzes, and other administrative tasks.




If your government activity is interested in hosting or if you desire to attend this video teletraining course, call **Cheryl Cross** at DSN 695-4390 or **Ray Yamaoka** at DSN 695-4893, commercial (804) 279-extension, for additional details.

# *WWW Security Program Assets*

BY WILLIAM L. UTTENWEILER, FSO
AEROSPACE CORPORATION, VANDENBERG AFB, CA

Newspaper headlines, always quick to focus on "bad" news, frequently remind readers of the dangers of the Internet. They report hackers defacing the World Wide Web home pages of major government agencies like the Department of Justice, the CIA, the Air Force, and NASA. They tell of viruses that destroy the information on unwary people's computers, including the Michelangelo virus and the Hare Krishna virus.

In addition, the early "netizens" were computer experts, many of whom had degrees in computer science and who understood the UNIX operating system. Computer security experts talk a language of their own—firewalls, spoofing, TCP/IP, etc.

Despite this, the World Wide Web has quickly established itself as an invaluable resource for security professionals. With only a few clicks of a mouse, a user can find the text of a misplaced Industrial Security Letter, the latest advisories for international travelers, security education resources from DoDSI or the National Counterintelligence Center, and updates to computer anti-virus software.

## Understanding the WWW

Many people are reluctant to venture onto the Web because they are confused by the terms used to describe the Internet.

The **Internet** is the network of computers linked by a high speed **communications backbone**. The basic technology was developed by the Advanced Research Projects Agency (ARPA) – now DARPA – in 1969 to provide a communications infrastructure which would survive a nuclear attack. The Internet exploded from a few computers in 1969 to 2,000 in 1985, and over 300,000 today. The technology has been both successful and widely copied. It was one reason American troops had so much trouble wiping out the Iraqi communications during the 1991 Gulf War.

At the heart of the system are the Internet Protocol (IP) and the Transmission Control Protocol (TCP). Since these two are used together, they are often referred to jointly as **TCP/IP**. The **IP** is the addressing scheme, which allows specialized computers called **routers** to move the information across the Internet. It converts a text name into the numerical address of the desired computer. **TCP** breaks large messages or data files into smaller **packets**. The packets are then sent over the network separately and reassembled at the destination.

The computers on the Internet have addresses which start with a **domain name**. Top-level domain identifiers give clues as to the nature of the entity which owns that computer. Table One shows what the top-level domain identifiers represent.

**Table 1**

| Domain | Signifies |
|---|---|
| .mil | Military |
| .gov | Government but not military |
| .edu | Educational institution |
| .org | Non-profit organization |
| .net | Network-related company |
| .com | Commercial firm |
| .ca | Abbreviation for a foreign country (in this case, Canada). Since Internet originated in the US, ".us" is not required. |

To the left of the domain name in an Internet address are one or more subdomain names. These identify the specific computer addressed. As an example, take my e-mail address: uttenweilr@vafb.aero.org. It indicates that I work for a non-profit company (true). "Aero" is the domain name for my company, the Aerospace Corporation. Within Aerospace Corporation's network, I am on the server named "vafb" (located on Vandenberg AFB, CA). By convention, we use our last name (or last name plus an initial) as the mailbox name. Mine is "uttenweilr" because the software only allowed for ten letters, and my last name is 11 letters long.

**E-mail** is a text message sent from one computer user to another, perhaps on the other side of the globe. It is "in the clear" like a postcard. Since it passes through other computers on its way to its recipient, outsiders (including hackers) at key points can intercept and read it. That is why people are wary of sending credit card numbers over the Net and some use encryption software to encode their messages.

Early Internet experts used programs like **telnet** to log into and work on a remote computer. Cliff Stoll made this process familiar to many security professionals in his book, *The Cuckoo's Egg.* In it, he described how West German hackers logged into American computers and tried to steal secrets for the KGB.

The **World Wide Web (WWW)** is a small part of the overall Internet. It relies on the **hypertext markup language (HTML).** This allows a programmer to associate text or instructions with either a picture or word(s) on a page. When a mouse pointer passes over text encoded in HTML, it usually changes into the form of a hand with a pointing finger. By clicking on that, a **hypertext transfer protocol (http)** command is sent over the network to request information. WWW addresses are called **universal resource locators (URLs).** The URL for my company's homepage is 'http://www.aero.org'.

When surfing the Internet, a user does not "log onto" computers in the sense that Cliff Stoll's hackers did. Instead, he or she sends requests for data, and the receiving computer transmits the information (words, graphics, etc.) to the requester's computer.

The program used to surf the World Wide Web is called a **browser.** The earliest ones included Lynx and Mosaic. Today's most common ones are Netscape's **Navigator** and Microsoft's **Internet Explorer.** Each allows a user to save the URL of homepages to which he or she expects to return as either **bookmarks** or **favorites.**

Commercial online services like America Online (AOL), CompuServe, and Genie sell the public access to information they have on their servers. Before the WWW developed so much easily accessible content, the commercial online services stood out for the information and services they offered. CompuServe strength was on-line discussion areas where computer firms answered questions from users. AOL distinguished itself with a large variety of chat rooms for online conversations, news, business, sports and travel, and games. A subscriber uses a phone line and modem to access the service's servers through special phone numbers. Subscribers or members of one of these services can send and receive e-mail from others with an Internet address.

People who do not subscribe to the service cannot participate in their chat rooms or forums and cannot view their content. When the WWW became so popular, these companies created links so subscribers could explore information on the Web, while keeping other Web users out.

Businesses often link their computer networks directly to the Internet. Individuals who want WWW access at home often do it through one of the proprietary firms like AOL, or through an **Independent Service Provider (ISP).** ISPs usually provide very little original content. What they offer is a quick connection to the WWW. ISPs are sometimes called Internet Service Providers.

At times, the WWW is so slow that it has been nicknamed the "World Wide Wait." A good analogy for understanding this phenomenon is a cross-country automobile trip. The time the drive takes depends on many factors – the speed of the car and congestion (or its absence) all along the route. For the WWW, these factors include the speed of the

network connection (a slow 14.4 kb modem or a fast T-1 line), the quality of the phone line (if the call is via modem), the congestion at the local server, the congestion on the net in general, and congestion at the destination server. Homepages with large graphics, sound, or animation files contain more content and thus take longer to download. The WWW generally slows down during evening hours, when people get home from work and log on. One of the worst delays occurred in November 1996. Thousands of people tried to access early election results at the All Politics site cosponsored by Time and CNN. As a result, very few got the information they wanted.

## Using a search engine

To find certain information, a user can type the URL into the browser and go directly there. For example, to find information about foreign travel advisories, the user could head for the Department of State's homepage at http://www.state.gov. From that page he or she can select the information from the choices offered.

However, just as people need a card catalog to find the location of a book in a library, so they need help finding information from among the 1,000,000+ sites on the WWW.

One method is to go to a Web site which has organized links to other interesting sites by their content. The first and most famous site of this type is **Yahoo!** By pointing the browser to http://www.yahoo.com, the user will find a menu of topics. Place the mouse pointer over a category, click, and the browser will offer links to sites of interest.

The other method is to use a **search engine**. This is a computer program which allows the user to insert a key word or phrase. It then searches through documents at sites throughout the WWW and reports back a list of "hits." The drawback of a search engine is that it will report thousands of hits for most key words. This flood of information overwhelms the ability of most users to select what is really needed.

Fortunately, the search engines allow for **advanced searches**. These use logical operators to refine the search and narrow the results. Some common logical terms are shown in Table 2.

**Table 2**

| Operator | Significance |
|---|---|
| "+" or "and" | Requires all words to be found. |
| "-" or "not" | Excludes article if a word is found. |
| "or" | Includes article if either word in a phrase is found. This is the default operator. |
| "near" | Requires two words be near each other (usually within 10 words). |
| " " | Placing words within quotation marks requires an exact match of the phrase. |
| * | An asterisk is a wild card. Searching for crypto* would report a hit for cryptography and cryptographer. |

Take a search for the keywords Aldrich Ames. The two words by themselves will result in many hits on documents from NASA's Ames Research Center in northern California. If '-NASA' is included, the NASA documents will be excluded. If quotes are used, only articles which mention "Aldrich Ames" by name will be found, but those with a middle initial will be excluded. This can be avoided by searching for: 'Aldrich NEAR Ames'.

There are many popular search engines. They include: www.yahoo.com, www.altavista.com, www.search.com, www.excite.com, www.dogpile.com, and www.lycos.com. Each search engine requires a slightly different gram-

matical structure in searches. Look for tips under **help, advance searches, frequently asked questions (FAQ),** or **search options** for site-specific tips.

One last tip about the WWW. It is much like a human community. New sites are born. They grow and mature. Sometimes they move from one place to another or change their names. They may become sick (communications or server malfunctions, hacker attacks, etc.). Documents are taken off servers to make room for newer information and sites close (die). More so than many other human endeavors, the WWW is characterized by constant change.

## What the future holds

In addition to the publicly available sites, an Intranet site (closed to the general public but open to insiders) is under development. Matt Donlon, Chief of the Security and Intelligence Office at the Defense Advanced Research Projects Research Agency (DARPA), has proposed development of a U.S. Government Intranet for the Security Professional (ISP).

The ISP is designed to allow government and industry professionals to quickly and efficiently interact on a wide range of issues. Donlon's list includes topics like security policy, threat information, training/education resources, visitor clearance, treaty information, and classification management.

The front door of the ISP would be open to the general public, like any WWW page. It would allow citizens to ask questions or voice their concerns.

However, only security professionals who had previously registered with the ISP would be allowed into the "trusted" FOUO level sections. There they could pass privacy data like Social Security numbers, birthdates, and clearance level data for visitor security clearances. Or they could take part in office of primary responsibility (OPR) moderated discussions about proposed security policy, like the on-going rewrite of the Automated Information Systems (AIS) chapter in the NISPOM.

The ISP might also act as a clearinghouse, so agencies that need a GSA-approved container might find a surplus one instead of having to purchase a new one. Companies could see what security forms and policies are already in use, eliminating the need to design new ones from scratch.

Donlon has developed a prototype site (http://isp.hpc.org) so Web surfers can get a taste of his vision. Among the agencies that have signed up to support the ISP's development are the Department of Energy (DOE), the Defense Intelligence Agency (DIA), the Defense Information Security Agency (DISA), the Defense Investigative Service (DIS), and the DoD Security Institute (DoDSI).

Once the basic ISP function is up and running, hopefully during 1997, Donlon predicts additional uses will emerge. For example, an on-line security library and an electronic expert consultation desk would allow quick answers to questions. Threat information and treaty response coordination could be provided in real time.

As Donlon sees it, technology can help the security community meet the challenge of Presidential Decision Directive #29. It can help to provide better security and modernize security management while reducing costs and increasing the security profession's credibility.

## Conclusion

The days of bookcases bulging with binders of paperwork are not gone yet. Their disappearance may still be years away. However the World Wide Web, with its volumes of easily available security related information and with the promise of trusted Intranets like the ISP, may be a tool to get security professionals closer to that dream.

# Making the Web Work
## Suggested Sites for Security Professionals

JOSEPH A. GRAU
DEPARTMENT OF DEFENSE SECURITY INSTITUTE

Knowledge is of two kinds. We know a subject ourselves, or we know where we can find information on it.

*Samuel Johnson*

The World Wide Web is a wonderful place, with tons of information available that can be useful to you as you manage your security programs. The problem is that there's *so much* available. The Web is a gigantic haystack with a sprinkling of worthwhile needles buried in it. In this article, I'm going to try to point you towards some Web resources that I think you'll find useful on the job. For each Web site, I'll give you the URL (the Internet address of the place) and a short description of what you'll find there.

We'll start with some sites dealing with security. (Makes sense, huh?) Then we'll move on to some other Web sites that don't deal specifically with security, but which provide a variety of resources you might find useful. I guess I should mention that most of these sites are maintained by commercial firms, non-profit organizations, or individuals. Listing them here does not constitute endorsement of the sites or their contents by DoDSI or the US Government. (There! That ought to keep the lawyers happy.)

How were these sites chosen? Basically, I tried to put myself in the place of someone managing a security program in an organization, and list sites that a person might find worth having at his or her fingertips. There was one other criterion .... Here at DoDSI, we access the Internet from behind a very finicky and cranky firewall. It blocks out Java, Javascript, certain types of imagemaps, and who knows what else! So the sites listed here are all sites that work well even if your Web access is pretty restricted technologically. They should be reasonably accessible to just about everyone.

Last item before we get to the good stuff .... If you find these sites useful and would like to keep them handy while you wander the Web, have we got a deal for you! On our DoDSI Web site, we have an abbreviated version of this article. (Less chatter, more matter.) It's set up in HTML as a stand-alone Web page. That means you can just add it to your bookmark or favorites file. We also have it packaged up neatly, so you can download it to your machine and set it up as the startup page for your browser, if you'd like. Just go to our site `[http://www.dtic.mil/dodsi/]` and look for the "Security Manager's Start-Up Page" link.

### GENERAL SECURITY SITES

Of course, we hope that our own Web site will be one of your favorite resources. On the site, we have course descriptions and schedules, electronic copies of some of our publications (with many more to be added as we can), a variety of reference documents, and information about the Institute. We're particularly proud of our "other places to visit" page, with (at last count) four dozen links to Web sites of interest to security professionals.

The DoDSI Web Site
`[http://www.dtic.mil/dodsi/]`

For folks involved with industrial security, there's plenty of useful information available at the Defense Investigative Service's site.

Defense Investigative Service
`[http://www.dis.mil/]`

The National Security Institute's Security Resource Net has an exceptional collection of on-line materials and links, covering a wide range of security interests.

National Security Institute's Security Resource Net
[http://www.nsi.org]

For people interested in the Information Security Program, there's a large amount of material at the Federation of American Scientists' Project on Government Secrecy page.

Project on Government Secrecy
[http://www.fas.org/sgp/]

This site contains information on recently issued security policies to include copies of the DoD 5200.1-R, "Information Security Program" and Change 3, DoD 5200.2-R, "Personnel Security Program."

The C3I Web Site
[http://www.dtic.mil/c3i/]

Posting current Security Policy Board actions and copies of security reports.

The Security Policy Board Site
[http://www.spb.gov]

## COUNTERINTELLIGENCE AND COUNTERTERRORISM AWARENESS

Postings on current foreign threats to U.S. business travelers and periodic newsletters.

The National Counterintelligence Center
[http://www.nasic.gov]

This site contains the FBI's program for the Awareness of National Security Issues and Response (ANSIR)

The FBI
[http://www.fbi.gov/ansir/ansir.html]

## COMPUTER AND INTERNET SECURITY

As you might expect, the most widely-covered security topic on the Web is computer security, with hundreds of Web sites devoted to all sorts of aspects of the problem. The National Institute of Standards and Technology provides a page with a tremendous wealth of resources, though it's a bit hard to wade through. Worth trying as a first stop on your search, though.

Computer Security Resource Clearinghouse
[http://cs-www..ncsl.nist.gov/]

The Library of Congress provides a page which focuses specifically on Internet security issues.

Internet Security
[http://lcweb.loc.gov/global/internet/security.html]

There are dozens and dozens of Web sites devoted to virus threats and countermeasures. This one -- from the Hitchhiker's Web Guide -- has a wide variety of information and material, and is organized so you can actually find what you're looking for.

Anti-Virus Resources
[http://www.hitchhikers.net/av.shtml]

Sometimes it's important for security folks to know what isn't a threat, as well as what is. In the myth- and misinformation-laden world of computer viruses, that's especially true. We need to be able to maintain our credibility in our organizations. Noted anti-virus expert Rob Rosenberger has an excellent page to help us do this.

Computer Virus Myths
[http://kumite.com/myths/]

## TIME

Need to know the exact time? The US Naval Observatory lets you access its master clock and find the exact time in all the US time zones.

US Naval Observatory Master Clock
[http://tycho.usno.navy.mil/what.html]

If you need to know the current local time across the country or around the world, try this page. Quick access to the correct time in 593 cities, worldwide.

The Time Zone Page
[http://www.webshaman.com/zone/]

## WRITING

If you're like me, you can never find your dictionary when you need it. No problem. Merriam-Webster's Collegiate Dictionary, Tenth Edition, is on the Web at this site.

WWWebster Dictionary
[http://www.m-w.com/cgi-bin/netdict]

If you need to look up a specialized, technical term -- in law, business, technology, computing, medicine, etc., try this page.

OneLook Dictionaries Home Page
[http://www.onelook.com/]

Roget's Thesaurus is one of the essential items in a writer's tool kit. It's available for searching here.

ARTFL Project: ROGET'S Thesaurus Search Form
[http://humanities.uchicago.edu/forms_unrest/ROGET.html]

Punctuation gives lots of writers problems. Craig Waddell of Rensselaer Polytechnic Institute has provided an excellent quick-reference tool on the Web.

Basic Prose Style and Mechanics
[http://www.rpi.edu/dept/llc/writecenter/web/text/proseman.html]

For answers to questions about grammar and word usage, try Jack Lynch's page. Lots of common-sense guidance.

Grammar and Style Notes
[http://www.english.upenn.edu/~jlynch/grammar.html]

## FOREIGN LANGUAGES

With international aspects of security being a major issue these days, being able to find the meaning of a word in a forign language may come in handy. This site provides translations of words from German, Dutch, French, Spanish, Danish, Finnish, Portuguese, and Esperanto.

Travlang's Translating Dictionaries
[http://dictionaries.travlang.com/]

English-Japanese and Japanese-English dictionaries are available at this rather amazing site created by Rafael Santos.

Japanese Language Information Files
[http://www.mickey.ai.kyutech.ac.jp/cgi-bin/japanese]

## TRAVEL HELP

Some of us travel a lot on business. Here's a site that provides custom maps and a route planner.

Maps On Us
[http://www.mapsonus.com/]

## TRAVEL OVERSEAS

Doing pre-travel briefings for members of your organization going overseas is an important aspect of our security education efforts. One very handy resource is the US State Department's Bureau of Consular Affairs page. Here you'll find the latest travel warnings and valuable Consular Information Sheets for just about any country you can think of, plus lots of other good information.

Bureau of Consular Affairs Home Page
[http://travel.state.gov/]

I've always thought it was a good idea to provide travelers with as much information as you can about their destinations and travel tips. Two reasons.... Helping them avoid health and other problems means they'll be at less risk of finding themselves in potentially compromising situations. Also, if we help them have a safe and hassle-free trip, they're more likely to come to us for briefings in the future. Besides, it's good PR for the security staff.

These two sites are first-rate sources of health-related information for travelers. The first is maintained by the Centers for Disease Control and Prevention; the other one is sponsored by the Medical College of Wisconsin.

CDC Travel Information
[http://www.cdc.gov/travel/travel.html]

International Travelers Clinic
[http://www.intmed.mcw.edu/ITC/Health.html]

To keep returning to the States hassle-free, you can check out the US Customs Service's excellent page of information for travelers.

Know Before You Go!
[http://www.customs.ustreas.gov/travel/kbygo.htm]

This next page has a variety of information, put together by a woman who is obviously a very savvy traveler. Check out the "Personal Travel Tips" section for some ideas you might want to share with your travelers.

Travel Kiosk
[http://www.afn.org/~afn11300/]

For general information about countries to be visited, the *CIA World Factbook* is a gold mine.

CIA World Factbook
[http://www.odci.gov/cia/publications/nsolo/wfb-all.htm]

Finally, here's a page with a huge collection of travel-related links, sorted by subject and by country.

NetTravel
[http://www.ypn.com/living/travel/]

## NEWS

Having good, up-to-the minute information about security issues and incidents can be a major plus for people doing security education. There are a wide variety of sources on the Web to tap. Here are a few particularly good ones.

Bob Drudge has put together a rather amazing collection of links to a variety of news sources: newspapers from all over the world, ABC, CBS, Fox, MSNBC network news, and more. This is probably where you'd want to start a search for news items of interest.

My Virtual Newspaper
[http://www.refdesk.com/paper.html]

For right-up-to-the-minute news, it's tough to beat the wire services. At the Fox News site, you have access to the lates stories moving on the Associated Press wires.

Fox News
[http://www.foxnews.com/news/]

The Cable News Network also provides a good source for up-to-the-minute news.

CNN Interactive
[http://www.cnn.com/index.html]

## SEARCHING

When you're looking for information about a specific subject on the Web (or the Internet as a whole), having the right "finding tools" at your fingertips can be a godsend. There are basically two types of finding tools: indexes and search engines. Indexes list URLs of pages dealing with various subjects, organized into hierarchies by subject matter. Search engines are large, searchable databases of URLs and related information. You type in search terms, and the engine lists pages for you which relate to those terms. There are many good indexes and search engines on the Web. We'll just list a few of the best.

Probably the biggest and one of the best Web indexes is Yahoo. You click on a category, then it gives you a list of sub-categories; click on one of those, and you get a list of sub-sub-categories. Work your way down through the pyramid, and you end up with a list of links to explore. Really good for when you don't know *exactly* what you're looking for. Yahoo also lets you search its database for specific terms. (Click on "options" beside the "Search" button to tailor your searching.) There are also separate, country-specific editions of Yahoo for Canada, France, Germany, the UK and Ireland, and Japan.

Yahoo!
[http://www.yahoo.com/]

Search engines are marvelous tools, but they can also be frustrating. It's almost an art to use them well -- to find just what you're looking for without being buried in a never-ending list of irrelevant sites. The secret is to look over the information provided by the engine about how it can be used, then experiment. Each engine has its own way of letting you tailor your searches to be most productive and efficient. Some use menus of search parameters, others have special search syntaxes (using things like quotation marks, capitalization, plus and minus signs), still others use both methods. As we look at the engines, I'll mention where you can find the help you need to make best use of it.

ZDNet has a really good article by Adam Page on how to use eight of the most popular search engines. It also covers the basics of something called Boolean searches, and gives ratings and descriptions of the engines. Definitely worth a look.

The Search is Over: The Search-Engine Secrets of the Pros
[http://www.zdnet.com/pccomp/features/fea1096/sub2.html]

One of the best of the search engines is AltaVista. It allows you to tailor your searches using either its own search syntax or Boolean search expressions. For the details on using these, click on "Advanced Search," then on "Help." AltaVista searches both the World Wide Web and Usenet newsgroups.

AltaVista Search
[http://www.altavista.digital.com/]

Another excellent search engine is HotBot. You can tailor your search by using HotBot's menus or with Boolean syntax. Click on "Help" for instructions. Searches the Web and Usenet.

HotBot
[http://www.hotbot.com]

There are also things called "multi-search engines." These gadgets let you enter search terms, then they go out and call on other search engines to find things for you. The best one of these I've found has a truly odd name: Dogpile. Don't let the name fool you, though; it's a very powerful tool. Dogpile searches the Web (using the Yahoo!, Lycos' A2Z, Excite Guide, World Wide Web Worm, WWW Yellow Pages , What U Seek, Lycos, WebCrawler, InfoSeek, OpenText, AltaVista, Excite & HotBot engines), Usenet (with Hotbot News, Reference.com, Dejanews, Excite News, Infoseek News, Altavista and Dejanews' old Database) and FTP sites (using Filez, FTP Search and Snoopie!). Click "Help with Syntax" to learn how to make the best use of this tool.

Dogpile
[http://www.dogpile.com/]

If it's a person you're looking for, there are search engines for that, too. Here's one that seems pretty good. (I tried five names on it the other day and it found five out of five.)

Switchboard
[http://www.switchboard.com/]

## WEATHER

There are quite a few weather sites on the Web. This one gives you plenty of information about weather in the States and overseas, and is pretty efficient about it.

Intellicast
[http://www.intellicast.com/]

## AND THEN THERE'S...

This last site in the list almost defies description. Bob Drudge has put together a site with pages full of links to reference material of all sorts. When you can't find what you're looking for anyplace else, try this one.

My Virtual Reference Desk
[http://www.refdesk.com/outline.html]

And that's the end of this short list. I hope you will find some of these sites useful in helping you make your security program a continuing success.

*introducing the industrial security professional's*

# Desktop Resource Guide

*a guide for Security Awareness Training and Education (SATE)*

First issued in 1994 and newly updated, the Guide is a user-friendly job aid package that provides valuable information for security professionals charged with implementing the security education requirements of the National Industrial Security Program (NISP) at their cleared facilities. The Guide provides

- **how-to guidance**
- **high-quality sample briefing materials**
- **up-to-date lists of resource providers of security awareness products and services**
- **briefing activities**
- **strategies for gaining greater management and employee involvement in the security program**

The Guide is based on the concept of sharing the "best of the best" SATE program ideas with others tasked with implementing the SATE requirements of the NISP. Based on the suggestions of Facility Security Officers, sample materials were collected from companies with excellent security programs. The best of the best were then selected for inclusion in the Guide.

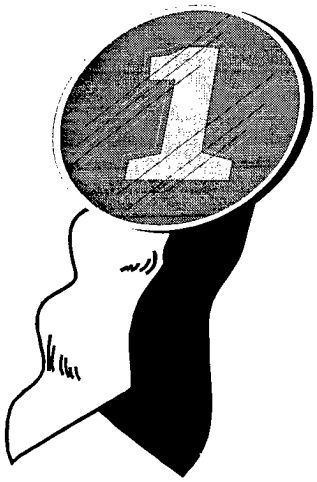
The Guide is available on software for use on a personal computer. This format allows users to easily reformat and modify the material for their own use. In addition, the software has been designed to help users navigate easily throughout the document. By simply pointing and clicking the mouse, users can go directly to specific topics, sample materials, or resource providers.

If you are a Facility Security Officer, contact your DIS Industrial Security Representative for a complementary copy of the Guide. The Guide will soon be available to government security managers from the Defense Technical Information Center and will be listed in their Nonprint Products Catalog. DTIC products may now be ordered through the DTIC homepage.

[http://www.dtic.mil/dtic/docorderform.html]

*This product was developed for the Defense Investigative Service by the Defense Personnel Security Research Center (PERSEREC).*

*Attention Security Educators, here's your chance to sign up for the:*



# Train-the-Trainer/Security Briefers Courses!

offered at the DoD Security Institute
in Richmond, Virginia, on:

| Train-the-Trainer | Security Briefers Course |
|---|---|
| June 23-27, 1997 | June 25-27, 1997 |
| September 8-12, 1997 | September 10-12, 1997 |
| January 26-30, 1998 | January 28-30, 1998 |
| April 13-17, 1998 | April 15-17, 1998 |
| July 20-24, 1998 | July 22-24, 1998 |

If interested in attending any of the above classes, please mail or fax us the Registration Form on the reverse. The fax is (804) 279-6406, DSN 695-6406. Address is DoD Security Institute, Attn: Registrar, 8000 Jefferson Davis Hwy, Richmond, VA 23297-5091.

If you'd like to *host* these courses, call Linda Braxton at (804) 279-6076, DSN 695-6076. If you have any questions about the courses, call Linda Braxton or Gussie Scardina, course instructor, at (804) 279-5308, DSN 695-5308.

## About the courses:

The **Security Briefers Course** (SBC) prepares security professionals to plan and deliver effective security briefings. Activities include preparing a briefing plan; presenting a briefing in a clear and interesting manner; designing and using briefing aids; and evaluating the effectiveness of an oral briefing.

The **Train-the-Trainer** for the SBC prepares security specialists to *teach* the Briefers Course. It begins as a two-day instructor preparation workshop before the first day of the SBC. The next three days are spent *teaching* the SBC under the supervision of DoDSI staff. Graduates return to their organization with instructor guide, student workbook, and handout packet. Activities include using the SBC materials, teaching the lessons in the SBC, assisting others to prepare briefing plans, and facilitating practice briefing sessions.

DoD Security Institute
8000 Jefferson Davis Hwy, Bldg 33E
Richmond, Virginia 23297-5091

# Registration Request

**To be officially enrolled, you must complete all information above the dark line.** In addition to serving as a permanent record of your registration, a class roster will be compiled prior to class from the information on this form. The roster will include your name, position, address, and phone number. If you have objections to this, please let us know. If you have any questions, call the Registrar (804) 279-4758, DSN 695-4758 (FAX 6406).

**Privacy Act Statement**

**Authority:** 5 USC 301 and DoD Directive 5105.42.

**Principal Purpose or Purposes:** The primary purpose served by DSI Form 2021A is to serve as a permanent enrollment record. Social security number (SSN) is required to distinguish between records of students with the same name.

**Routine Uses:** DSI Form 2021A is routinely used as an alphabetical index and locator card for students and as a course completion record.

**Disclosure:** Disclosure of information, including SSN, is voluntary. Failure to provide such information could result in inaccurate records of students with same name.

Course title | Course dates

Mr. / Mrs. / Ms. | Name (Last) (First) (MI) (subtitle: Jr., III, etc.)

Social Security Number | Position

Agency/Activity Code (see reverse for codes) | Mil Rank/GS Grade/Contractor | Gender M F

Duty station/Facility address | Name of Supervisor

(city) (state) (zip) | DSN: | Commercial:

DSN:

Commercial No.

Fax:

**DoDSI supports the Americans with Disabilities Act of 1990. Attendees with special needs should indicate those needs here, or call (804) 279-4758/4892.**

**Attendance approved by official? (if identified in the course description sheet) Yes No**

**Agency/Activity:** (If your agency is not listed, please write it out.)

| | | | | | |
|---|---|---|---|---|---|
| DAF | Air Force | DJT | Joint Command | OFE | Federal Emergency Mgmt. Agcy. |
| DAY | Army | DMC | Marine Corps | OFG | Foreign Govenment |
| DSA | Defense Info. Systems Agency | DNY | Navy | OJU | Justice Department |
| DIA | Defense Intelligence Agency | DSD | Secretary of Defense | ONR | Nuclear Regulatory Commission |
| DIS | Defense Investigative Service | DoD | Other Department of Defense | OST | State Department |
| DLA | Defense Logistics Agency | OED | Education Department | OTP | Transportation Department |
| DMA | Defense Mapping Agency | OEG | Energy Department | OCP | U.S. Capitol Police |
| DNA | Defense Nuclear Agency | OEP | Environ. Protection Agcy. | IND | Private Industry |

# From a Culture of Secrecy to a Culture of Openness

## A review of the Report of the Commission on Protecting and Reducing Government Secrecy, 1997

BY LYNN F. FISCHER, DOD SECURITY INSTITUTE

The *Report of the Commission on Protecting and Reducing Government Secrecy*[1] has just been published and is viewed by many as the most comprehensive study of government security policy and practice available at this time. It deserves the full attention of security professionals who look to the national legislature for long-term direction and possibly for a solution to the crisis in confidence faced by the Federal Government, resulting from the costly proliferation of classified documents in the past three decades of the Cold War era.

The stated objective of the Commission as eloquently spelled out by its Chairman, Senator Daniel Moynihan, is to move from a culture of security in government (where what is not secret is easily disregarded or dismissed) to a culture of openness where valued information is used to the full benefit of the public. And how would this come about? The report contains many recommendations, but the central argument is that the government-wide system of classification, declassification, and access to classified information should be based on a new law rather than departmental and agency regulations. With the exception of the Atomic Energy Act of 1956 which provides a statutory basis for the protection of information concerning atomic energy, our information and personnel security programs are based on regulations derived from presidential orders.

### Six principles for proposed legislation

To some, the report sounds like a indictment of Federal security programs. But we should keep in mind that it was researched and written within the context of the American constitutional system of separation of powers in which there is a natural and healthy tension between the executive and legislative branches of government. The Commission, as an initiative of Congress, has exercised its license to critically evaluate what executive agencies have undertaken up to the present based on regulation. The writers do acknowledge that in the past two years, with the issuance of two important executive orders and the establishment of the Security Policy Board to coordinate federal-wide policy, many of the issues raised by the Commission have already been addressed. Nevertheless, they urge that new legislation should be enacted as a check or control against excessive classification and costly activities for which there is no value-added. The report prescribes six essential features of the proposed legislation:

1. Information should be *classified only if there is a demonstrable need* to protect it in the interest of national security with the goal that classification is kept to an absolute minimum consistent with these interests.
2. The President should establish procedures and structures for classification of information and for a parallel program of declassification.
3. Standards and categories to apply in determining classification should include consideration of *benefit from public disclosure* and weigh it against the need to have it or keep it classified.
4. Information should remain *classified no longer than ten years* unless, based on current risk assessments, an agency certifies that the information requires continued protection. All information would be automatically *declassified*

[1]See the *Security Awareness Bulletin,* 1-96, "A New Look at Government Secrecy," for an introduction to the work of the Commission.]

*after 30 years* unless it can be shown that harm would result from its release. Systematic declassification schedules should be established with annual reports to Congress from agencies on classification and declassification programs.

5. The statute would not be construed as an authority to withhold information from the Congress.
6. Congress should establish a National Declassification Center to oversee declassification practices by the Federal Government. The Center would report annually to Congress and the President on the status of declassification.

## Recommendation highlights

The report offers sixteen formal recommendations and several informally stated proposals. Several of these concern organizational structures and administrative procedures. Some are of particular interest to our readership of security educators. Others address specific problems that the Commission believes need fixing. Here are a few highlights from the list of formal recommendations that zero in on what the commission sees as specific problems. It is proposed that:

- The Security Policy Board establish a single set of security standards for special access programs.
- Original classifiers provide a detailed justification for each original classification decision.
- Derivative classifiers be required to identify themselves on the documents they classify.
- The use of sources and methods as a basis for the continuing classification of intelligence information be clarified by the Director of Central Intelligence.
- Agencies establish ombudsman offices in each agency that would intervene in and resolve classification and declassification issues and act as a conduit for public concerns about access to records.
- Individuals in both Government and industry holding valid clearances be able to move from one agency or special program to another without further investigation or adjudication.
- Congress and the Executive Branch reevaluate the requirement to utilize a new financial disclosure form and consider staying its implementation until there is further evaluation concerning how it would be used and whether its benefits exceed its costs.
- Development of an information systems security career path across the government.

Of more general interest is that the Commission, in addition to recommending a legislative basis for security policy, calls for the assignment of all classification and declassification policy development and oversight to a single Executive Branch body with sufficient resources and authority to carry out oversight of agency practices. Furthermore, the report calls for a National Declassification Center at an existing Federal agency to coordinate declassification policy and activities. All of this is proposed as a means to improve Executive Branch policy development and oversight.

## A call for risk management

Throughout the Commission report we see the influence of *risk management philosophy* originating in the Joint Security Commission's 1994 report.[2] The present report carries the concept further by arguing for sensible risk management as an integral part of deciding whether information should be classified. One of its formal recommendations states that "Additional factors [in addition to potential harm from release] such as the cost of protection, vulnerability, threat, risk, value of the information, and public benefit from release, could also be considered when making classification and declassification decisions.

The concept of risk management is also strongly endorsed with regard to personnel security: In this era of diminishing personnel security resources, the report states we should reduce inefficiencies in the processing of cases by applying risk assessment principles. For example, the commission proposes

[2] The Report of the Joint Security Commission issued in February 1994 called for balancing the risk of loss or damage of disclosure against the cost of countermeasures, and selecting a mix that provides adequate protection without excessive cost.

expedited processing of non-issue cases in the granting of clearances. Also in line with risk management, it recommends that standard requirements for neighborhood interviews and the interviewing of educational references be dropped from background investigations. Research, they maintain, has shown that these very costly methods have the least payoff in terms of gaining productive information about clearance applicants.

## The need for continuing evaluation

Conversely, since the study of contemporary espionage shows that most espionage offenders – U.S. citizens having access to classified information – turned to espionage *only after several years of service in a position of trust*, the Commission report argues for establishing a greater balance between the initial clearance process and programs of continuing evaluation of cleared employees. It states that greater attention needs to be directed toward making continuing evaluation programs more effective. It proposes monitoring the behaviors and activities of cleared personnel in a cost-efficient and non-intrusive manner.

Echoing the language of the Executive Order on Access to Classified Information (EO 12968), the Commission gives a strong endorsement to the strengthening of employee assistance programs (EAPs) and extending these programs to all cleared contractor employees. The report states, "While the number of individuals who did not commit espionage as a result of successful counseling is impossible to quantify, helping cleared employees cope with their personal problems almost certainly will deter some incidents of espionage and other major security breaches."

While the Commission report contains the strongest possible endorsement of monitoring and continuing evaluation programs, it fails to address the role of security awareness on which continuing evaluation depends. Essential to this type of program is the proactive support of motivated and knowledgeable co-workers and supervisors. It appears that we have to read between the lines: If employee assistance programs are important, employees of course need to be informed about them and the confidentiality that they offer to those seeking help. Also, awareness of appropriate reporting procedures for situations in which a co-worker witnesses suspicious behaviors or security infractions are also essential to the continuing evaluation concept. The security professional in his or her role of educator is in fact the lead actor in ensuring that persons already in a position of trust are provided the motivation and collegial support to *remain trustworthy.*

## Of special interest to the security educator:

In other areas touching on the necessity for security education, however, the writers of the report do not let us down. Four important recommendations emerge from the discussion which deserve our attention:

***a. Training for derivative classifiers.*** In a lengthy section entitled "Improving the Training and Education of Classifiers," the report calls attention to the mandate of Executive Order 12958 which states that original classifiers must "receive training in original classification." The commission notes, however, that the order does not set minimum standards for this training and finds, regrettably, that there are no plans to consider such standards.[3]

But this is not all. In a proposal aimed at improving the quality of classification decisions, *the Commission recommends expanding the mandated training in the executive order to include derivative classifiers*. Since over 90% of all classification actions are derivative and virtually any cleared employee in government or industry has derivative classification authority (estimated at three million), this would be an awesome undertaking. However, given the exacting requirements of the new executive order for marking derivatively classified documents with data from original sources, the

[3]The Department of Defense Security Institute has developed and distributed over 2,000 copies of an Original Classification Authority (OCA) training package throughout DoD agencies and military departments. The package, which is intended to be placed with each OCA, includes a set of pamphlets and a short video, "The Thinker." We invite requests from any OCAs who have not received a package. Please fax us at DSN 695-6406 or commercial (804) 279-6406.

commission concludes that personnel must have that training if the requirements set by EO 12958 are to be met. [4]

***b. Enhanced threat awareness regarding information systems.*** One of the clearest calls for putting more resources into security education and awareness has to do with providing information about the threat to information systems – computers and networks now being routinely attacked and frequently penetrated by hackers. Of course what we are really worried about here are intrusions by cyber-terrorists or an adversary which might pull off an electronic Pearl Harbor through disruptions of military operations or denial of service to deployed U.S. forces.

With regard to the dissemination of threat information, the reports states that there is at present no national-level computer incident response center that is able to receive and analyze attacks, denials of service, or computer crime. And there is no systematic means for informing agencies or private industry about threats to the National Information Infrastructure. The report concludes that the necessary resources must be dedicated to eliminating these deficiencies.

***c. Training for all users of Government computers:*** Under the chapter entitled, "Information Age Insecurity," the Commission identifies improved education and awareness and training as one of several critical means for improving information systems security. Other factors are greater executive branch and congressional oversight and upgraded capabilities for responding to emerging threats. When planning for the future, the report states, one of our highest priorities should be continuing education for senior executives, *all users of federal computers*, and overseers of information systems security who "need continuing education and training to remain abreast of development information systems technology and understand how to protect the contents of those information systems." The writers identify three elements to this training: basic rules for the use of information systems, security awareness related to threats and vulnerabilities, and automated and accessible information exchange.

***Definitions***

*Original classification*: An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure. Individuals having original classification authority are authorized in writing either by the President, by agency heads, or other officials designated by the President, to classify information in the first instance.

*Derivative classification*: The reproduction, extraction or summarization of previously classified information from original sources and applying appropriate markings derived from source materials.

The writers contrast this recommendation with present reality: Citing a 1996 survey of Federal agencies, the Commission found that few employees had even a working knowledge of current laws about the misuse of computer systems and that there is no coordinated Federal Government effort to teach computer ethics or rules of behavior for users of government-owned systems. As the report points out, however, standard and required training for all government users, which was much earlier prescribed by the Computer Security Act of 1987, amounts to an unfunded mandate since the act did not include budgeting requirements to cover training costs. We would add that as computer usage is near universal, this would be an additional monumental training requirement. The report does point to a possible solution—automated or computerized training courses.

[4] In fact, training standards for both original and derivative classifiers have been established in *Directive No. 1, Classified National Security Information, Subpart D – Security Education and Training.* This implementing directive for Executive Order 12958 was issued by the Office of Management and Budget, Information Security Oversight Office, effective October 14, 1995, and reprinted in the *Security Awareness Bulletin*, 1-96, May 1996. In addition, the Training and Professional Development Committee of the Security Policy Board has developed generic training packages for original and for derivative classifiers. These packages are in the final review stage.

*d. The development of the Intranet for Security Professionals.* The third element of education and training, also of great significance to the security educator, is accessible information exchange. As potentially the most promising method to achieve this objective, the Commission gives a ringing endorsement of the development of the Intranet for the Security Professional (ISP) by the Defense Advanced Research Projects Agency. (See the article on the ISP in this issue.) Information exchange through the Internet or the ISP in the future will operate as an invaluable conduit for information on products, methods, and educational content and policy guidance.

## What wasn't said in the Commission Report

Quite appropriately, the authors identify the limits of the Commission's inquiry. They admit that there are many security issues not addressed in its report, including physical and technical security measures used to safeguard information, secrecy in the Judicial and Legislative Branches, the impact of government security requirements on the private sector, issues related to the roles and missions of intelligence organizations, and the protection of personal privacy.

But there are other unsatisfied concerns: A senior consultant on security issues, while praising the report in general, nevertheless expresses disappointment that the Commission failed to deal with the question of sensitive but unclassified information – including militarily significant technologies on which our military strength and economic viability may depend. Mr. James Bagley, states that "an important, but frequently misunderstood question as to whether Unclassified equals Public information was not adequately discussed in the Report." Bagley points out that there continues to be a misperception that once classification caveats are removed, information (technical or otherwise) automatically becomes 'public information.' This is not, nor should it be, the case. [5]

Others wonder whether anything will come of this work in terms of legislation or significant change. Public interest advocate and frequent critic of government security policy, Steven Aftergood, writing in the *Secrecy & Government Bulletin* comments that "a report, even a superb report, does not in itself change anything [but this one] deserves the attention of everyone who is affected in some way by government secrecy, which is just about everyone."

## The report as core literature for the security professional

Quite apart from the merits or weaknesses of any of the Commission's recommendations is the value of this document as important background literature and reference document for the serious security professional. We have under one cover a review of the history and philosophy of information and personnel security in the 20th century – where we have been in this discipline and where we may be going. Appendix A (86 pages): "A Brief Account of the American Experience," authored by Senator Moynihan, offers fascinating reading. Both the Chairman's Forward and the Vice-Chairman's Forward (by the Honorable Larry Combest, U.S. Representative from Texas) cover the recent history of government regulation and contemporary thinking on the "statutory solution." Embedded in the report itself are insightful discussions of the problems and issues facing the security and intelligence communities in this decade and proposed solutions to those problems. In all, this is a textbook from which we as students and practitioners can all benefit.

## How to get a copy of the full report

Bound versions of the report are for sale by the U.S. Government Printing Office, Superintendent of Documents, Mail Stop: SSOP, Washington DC 20402-9328. Their order desk number is (202) 512-1800; order fax number is (202) 512-2250. Cost is $25.00 and the stock number is 052-071-01228-1. The full text of the report can also be downloaded from the World Wide Web at

`[http://www.access.gpo.gov/congress/commission/secrecy/index.html].`

[5] From and unpublished assessment of the Commission report by James J. Bagley, President of R.B. Associates of Falls Church, Virginia.

## Downlink DoDSI presents

# *"Protecting Classified National Security Information"*

The Information Security Team of the Department of Defense Security Institute (DoDSI) will beam a **video teletraining course** to classrooms across the United States on the following dates:

| 1997 | 1998 |
|---|---|
| **22 - 24 July** | **21 - 23 January** |
| **30 September - 2 October** | **28 - 30 April** |
| **18 - 20 November** | **25 - 27 August** |

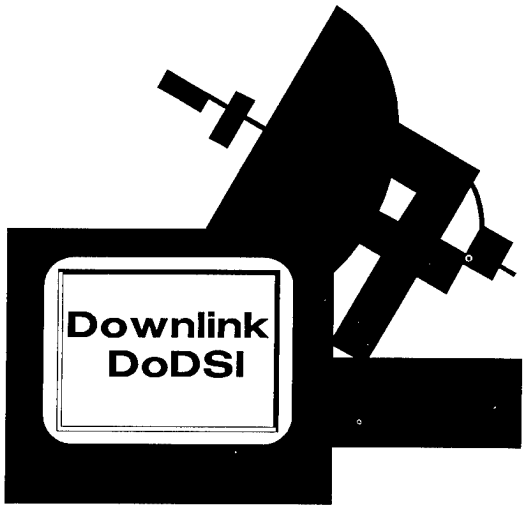
If your installation has a satellite downlink (it probably does), then you can subscribe to this training opportunity. Video teletraining is a highly cost effective alternative to on-site, instructor-led training. If your training budget requires creative alternatives, video teletraining may be the solution. This training will be presented at no charge to the receiving activity.

The training will take place over three-days and was created specifically for television. It provides the **basic requirements** for personnel with routine access to classified information.

Students at your site will interact live with DoDSI instructors at Fort Lee, Virginia, via the Satellite Education Network (SEN) to learn the answers to these questions:

- What is classified information?
- Where does it come from?
- What's the correct way to

| | |
|---|---|
| Mark it? | Handle it? |
| Process it? | Control it? |
| Store it? | Transmit it? |
| Destroy it? | |




The students will learn the latest changes to the program and how they affect your organization. If your government activity is interested in hosting this video teletraining course, call **Cheryl Cross** at DSN 695-4390, commercial (804) 279-4390, for additional details.

# Empowering the Security Educator with Products and Resources....

## *through the Center for Security Awareness Information*

Jointly sponsored by the Department of Defense Security Institute and the interagency Security Awareness and Education Subcommittee, the CSAI was created to support security awareness activities throughout government by providing information about educational products and resources and by facilitating their low-cost distribution.

If you as a security professional with briefing or educational responsibilities for an employee population or personnel in a military organization have felt hard-pressed to deliver the security message to a sometimes skeptical and hard-to-sell audience, take heart. You are not alone! However geographically or organizationally isolated you may be, there is a community of like-minded professionals faced with the same challenges (and usually with the same limited resources). By sharing information, quality awareness products, and other resources to support educational activities, we can collectively accomplish the task of convincing our personnel that the threat is still there and that good security practices can keep this country strong and our economy viable.

The ***Center for Security Awareness Information***, now about two years old, is one community-wide activity that can do this. The CSAI is essentially a product and resource information clearinghouse which depends upon input from everyone who has something of value that can be shared. Its primary vehicle for providing this information to the community is:

The ***Announcement of Products and Resources,*** published approximately every six months with the addition of new and up-to-date product information.

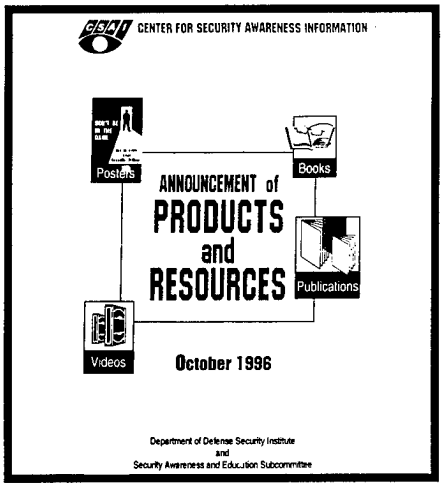
**There are two ways to get this publication:**

- The March 1996 edition is available as a downloadable document from DoDSI's homepage:

  `http://www.dtic.mil/dodsi`

This will require the use of an Acrobat Reader which is itself downloadable from our Web site.

- If you do not currently have Internet access, we will send you a hard-copy by mail. Just fax us a request at the DoD Security Institute: (804) 279-6404 or DSN 695-6406.



## *This is how the CSAI works:*

*Product Identification:*

Security professionals throughout the federal agency and contractor community send us a copy or alert us about the production of new, good quality products – videos, posters, publications, briefing packages, etc. – that have a potential for broader use beyond the organization which produced them.

*Product Review:*

Once a product and its source are identified, we undertake some method of product review and profiling to come up with a description that will help a potential user in making a decision as to whether or not a product will meet the educational objectives for a specific target audience. Actively involved in the review process are members of the SAES at its monthly meetings and DoDSI professional staff, with the help of test audiences made up of resident course students in Richmond, Virginia.

*Reproduction and Broader Distribution:*

Based on the outcome of the product review and our estimate of its potential demand in the larger security community, decisions are made about how it can be produced in larger quantity and distributed. Sometimes the originating organization has the resources to undertake a wider distribution, sometimes we can arrange support from another agency or cooperative group, or put in place a method by which requesters pay a minimal cost for reproduction, processing and shipping. Whatever arrangement is decided upon, information about how to obtain that product will be included in announcements and listings.

*Advertising and Listings:*

The main vehicle for product and resource information will continue to be the ***CSAI Announcement of Products and Resources***. Special notices of new products and their availability will routinely appear in the *Security Awareness Bulletin*, which has been a regular source of new product information since its first publication in 1981. In the *Bulletin's* web-site edition, which up to the present time has provided only feature articles, we will now include all product and event announcements for the current issue in Adobe Acrobat format.

***Benefits to the Security Community:***

There will be two obvious major benefits to security educators: First, we will all enjoy faster and more comprehensive access to better quality products. Secondly, by giving greater exposure to effective products, we will be saving money, a fact to share with your management. Economics would call this benefiting from economies of scale; security professionals are more likely to say that we've stopped reinventing the wheel and the costs that come with constant

reinvention. It amounts to the same thing: If one agency or firm develops a great (for example) foreign travel briefing in video or CBT format that can be used by others, consider how cost-effective that product could be. If the initial investment in product development is $40,000, that is a savings of $40,000 many times over that other organizations don't have to spend to meet the same awareness objectives. Plus everyone will have unlimited use and benefit of a high-quality product.

You now have at your fingertips (or at ready access) product and support information that will make your educational duties more effective and rewarding to yourself and to the people who need the security message.

---

A sample page from our most recent edition of the ***Announcement of Products and Resources***, October, 1996, follows on the next page. This page is from *Section 3 Product Profiles: New and Current Videos*. Each product which is listed for the first time is identified as NEW so that the listing can be easily spotted by the user.


## SOMETHING WASN'T RIGHT!

***Subject Focus:*** Personnel Security, Espionage, and terrorism

***Release Date:*** 1996 ***Run Time:*** 18:00

***Producing Organization:*** National Counterintelligence Center in conjunction with FBI, and DOE

***Intended Target Audience:*** Government and industry security community

***Classification/Limitations:*** Unclassified

***Availability and Cost:*** To obtain a VHS copy of this product, send $9.95 (pre-paid) or a government purchase order for $29.95 to CopyMaster Video Inc., Department 15, P.O. Box 684, 711 Fairfield, Villa Park, IL 60181, phone (630) 279-1276

***Description:*** This video was developed to encourage aware and conscientious employees in government and industry to overcome their inhibitions to reporting suspicious behavior to appropriate security officials. The video features three significant cases: The capture of FALN members in Evanston, Illinois, the Pollard espionage case, and the U.S. Customs Service investigation of Dr. Ronald Hoffman

***Test Audience Assessment:*** The test audience consisted of students at the DoD Security Institute enrolled in the Information Security Specialist Course in April 1996. The test audience gave this video extremely high ratings with respect to suitability and technical accuracy. The video is not geographically limited or dated. It was also viewed as being sensitive from the standpoint of propriety - 40 percent of the test audience gave the video positive marks for portraying human relations in a positive manner. Over half of the evaluators rated the video's production quality as high. The video was judged to be high in clarity, credibility, use of time, and suitability for all audiences. It's production quality, ability to hold an audience's attention, constructive tone and impression, and flexibility also received high marks.

**re-scheduled**

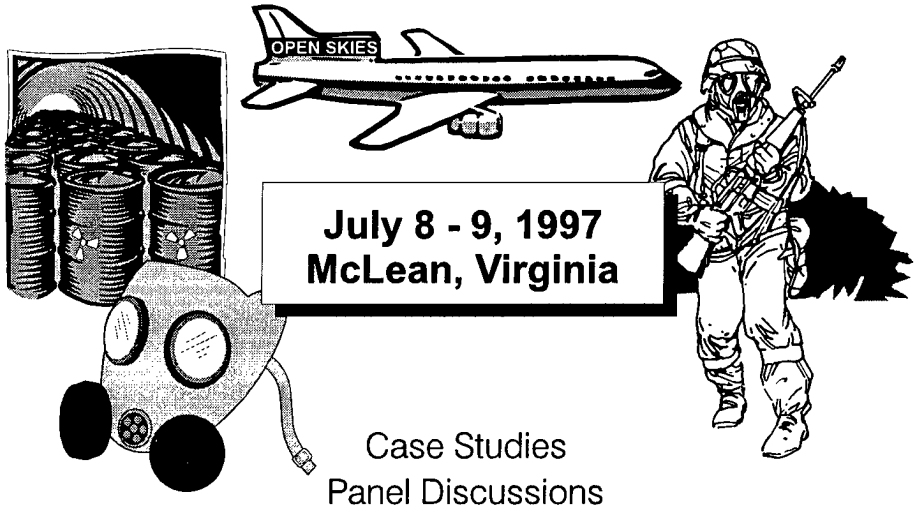
Defense Treaty Inspection Readiness Program

# NATIONAL SEMINAR

Focus of this year's seminar
is the

## Chemical Weapons Convention

Entry Into Force 29 April 97




**July 8 - 9, 1997**
**McLean, Virginia**

Case Studies
Panel Discussions
Facility Negotiations
Technical Equipment Issues
Arms Control Security Overview
Chemical Weapons Convention Overview
CWC Challenge Inspection/Managed Access

**To register or for more information call: 1-800-419-2899**
**or visit the DTIRP homepage @ www.OSIA.mil**
**U.S. Confidential clearance required for attendance**

## ATTENTION: Facility Security Officers and Security Staff

The *FSO Program Management Course (FSOPMC)* is presented, in conjunction with the Defense Investigative Service, in numerous cities around the U.S. each year. It is one of the oldest, most popular courses presented by DoDSI and there is often a waiting list.

To give you more opportunities for this training and reduce some of the costs, we have developed a video teletraining version of *FSOPMC*. The teletraining system "beams" the instructors live into your local classroom or conference center onto a television screen via satellite. With microphones and communications equipment, each student can participate in discussions or ask questions and get immediate answers from the instructor. Additionally, we hope to setup high speed telephone line connections to locations that can not pickup the satellite signal.

### About the course

*FSOPMC* is a three-day course designed to give a basic understanding of the National Industrial Security Program (NISP) and, more specifically, the National Industrial Security Program Operating Manual (NISPOM). Topics include facility clearance and changed condition, classification management, safeguarding and personnel clearance procedures. DoDSI will continue presentations of the course onsite in addition to the teletraining.

The video teletraining version of the *FSOPMC* also lasts three days. Each day will consist of four hours of video teletraining and two hours of activities led by an onsite expert as the facilitator. The activities include practical exercises, quizzes, workshops, etc. These activities enhance, reinforce, and provide practical application for material introduced by the broadcast.

## *Downlink* DoDSI FSO Program Management Course

We are planning the first broadcast for September 1997. Students successfully completing either version of the course will receive a certificate of training which will satisfy the FSO training requirement of the NISPOM.

### About the technology

We call our video system "Downlink DoDSI" and currently broadcast over the Satellite Education Network, a part of the Government Education and Training Network. Broadcasts originate from studios at the Army Logistics Management College, Fort Lee, Virginia. The signal is sent to receiving sites via the Telstar 402 satellite. Audio from each site goes by telephone line to the studios in Virginia, giving real-time voice communications. (See next page for more technical talk.)

### Getting hooked on video

To help figure out the best arrangements to reach you, ***please let us know if***:

- *your location uses video teletraining or has a location near by where employees normally go to use it,* ***OR***
- *your technical people believe you can connect to "Downlink DoDSI" (as explained in the technical information on the next page) and who we should call for more information,* ***OR***
- *you want to receive the course via video*

Please send us that information along with your name, phone number and facility address. You can reach us by fax ATTN: INDST at (804) 279 5239 or email it to INDST@dodsi.dscr.dla.mil. To phone your response or get more information or help call Mike Black at (804) 279 4187 or Mike Marcolivio at (804) 279 5310.

# *Downlink* DoDSI: Technical Information

DoDSI broadcasts from the Satellite Education Network (SEN) at Ft. Lee, VA. SEN is part of the Government Education and Training Network (GETN) established with AT&T Tridom. GETN is a consortium of federal agencies training by one way video/audio via satellite and return audio via ground link through Tridom. Tridom representatives are Jolly Holden, Manager, (770) 514-3797 and Bob Bland, Engineer, (404) 810-8680 or (770) 514-3390. Use of the broadcast requires prior acceptance by DoDSI to assure it can support the training.

There are over 900 GETN downlink sites in the U.S.; the largest number of which Department of Defense operates. The sites are equipped with a Ku-band antenna. They receive the broadcast in digital, 3.3Mbs compressed format from the Ku-band transponders of the Telstar 4 satellite (previously named Telstar 402). Telstar 4 has a geosynchronous orbit located at 89 degrees W.L. and provides 60 to 120 watts per transponder. Additional technical data on the satellite and its orbit can be obtained online at www.att.com/skynet. At times, DoDSI broadcasts are simulcast over TNET, a VTEL two way video/audio training network operated by the Army.

GETN uses CLI CODEC (Coder/decoder) to scramble/descramble and compress/decompress the signal. The CLI decoder at each site has a serial number that is registered with Tridom. Only the registered decoder at sites authorized by SEN can successfully process the signal. GETN and TNET facilities may be located near some contractors; however, their use would have to be individually arranged. DoDSI will post a listing of SEN and TNET sites to its web page at www.dtic.mil/dodsi/prodsvcs.html under "Training by Satellite." The Federal Government Distance Learning Association web page, www.fgdla.com, also has some GETN information. Similar information is available from SEN at (804) 765-4512/4004 and TNET at (757) 878-4210.

Besides using an available GETN or TNET facility, contractors have several options to receive the signal at or near their location.

**Direct Receive from Satellite** Requires (1) available facility for broadcast dates; (2) steerable digital Ku-band antenna with a Low Noise Block Converter or antenna otherwise locked on Telstar 4; (3) the CLI decoder (which, if you don't have, could be leased/rented); (4) registration of the decoder serial number at Tridom; and (5) the site be authorized for the broadcast (have the decoder recognized by the system and logged in through SEN/Tridom for the broadcast).

**Terrestrial Connection** If the site can connect its video system to the public telephone system, then the signal can be sent to that location via telephone lines at 384 kbs (equivalent of 1/4 T1 or ISDN PRI). This will require a corresponding line capability and CODEC device at the site to handle the receive and send signal over the phone lines. Highest quality transmissions will occur when the CODEC at the receive and send sites are the same or made by the same manufacturer and are fully compatible. Otherwise, the signal would use the industry standard H320. DoDSI would have to arrange for retransmission of the signal. That could be over the Army's TNET which uses VLI CODEC and video conferencing equipment. TNET would connect to the receive site through its center or through Sprint. Availability of this option will depend on cost to the government.

**Commercial Services** Contractors may elect to connect their video system to commercial service or use a commercial facility. The receiving contractor would have to bear the added costs. Listings of video conferencing sites is available from the International Teleconferencing Association (ITCA) at www.ITCA.org in the "Reference Library" under "Conference Room Directory."

**Analog Satellite Signal** SEN has the capability to send an analog signal as well as its normal digital signal, using the Telstar 4 or some other satellite. The analog signal will be in the clear, uncompressed, and receivable by an antenna locked on the relaying satellite. SEN would have to complete the arrangements and publish the satellite and transponder identification in its schedule. The receive site would need a steerable antenna, normally C-band, unless it happened to have its antenna fixed on the selected satellite. Availability of this option will depend on cost to the government.

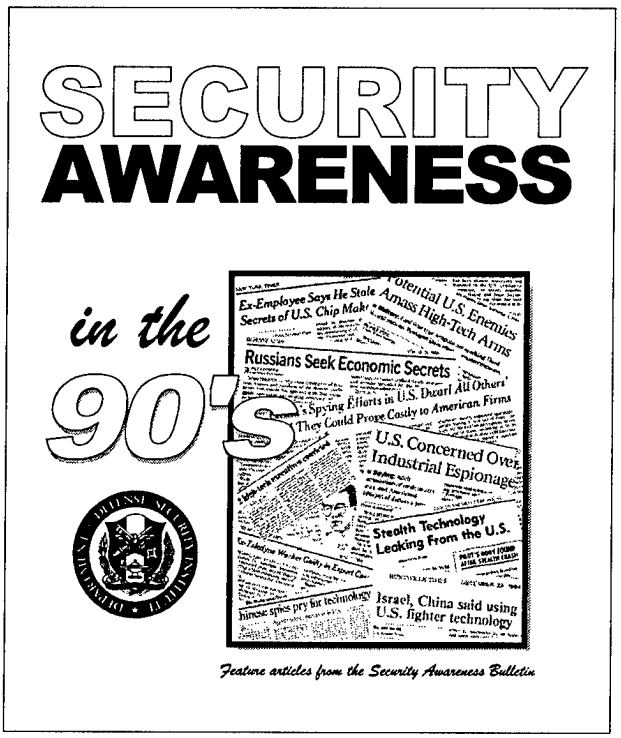
For any of these options, there would be an audio bridge back to SEN via telephone through Tridom.

# Security Awareness in the 1990s

feature articles from the
*Security Awareness Bulletin* 1990-1996

Subject areas:

- the foreign intelligence threat
- espionage case studies
- industrial security
- information systems security
- security policy and programs
- the threat to U.S. industry




*Feature articles from the Security Awareness Bulletin*

This is the second compilation of past *Bulletin* articles issued by the DoD Security Institute. The first volume, Security Awareness in the 1980s, was published in 1990 and was an immediate success. The new edition picks up where the former left off. It will be particularly useful to younger security professionals who didn't see these articles when they first appeared.

.....

Superintendent of Documents **Publication** Order Form

Order Processing Code
*8012

Credit card orders are welcome!

Fax your orders (202) 512-2250
Phone your orders (202) 512-1800

___ copies of **Security Awareness in the 1990s,** S/N 008-047-00409-5 at $22.00 each ($27.50 foreign).

The total cost of my order is $ _____. Price includes regular shipping and handling and is subject to change.

Name or title (Please type or print)

Company name Room, floor, suite

Street address

City State Zip +4

Daytime phone including area code

Purchase order number (optional)

Check method of payment:

☐ Check payable to: Superintendent of Documents

☐ GPO Deposit Account ☐☐☐☐☐☐—☐

☐ Visa ☐ MasterCard

☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

(expiration date)

☐☐☐☐

*Thank you for your order!*

Authorizing signature

Mail to: Superintendent of Documents, PO Box 371954, Pittsburgh PA 15250-7954

# *Security Awareness Bulletin*

## Subscription Service

As we announced in our last issue, beginning with the first quarter of 1997, the *Security Awareness Bulletin* can no longer be distributed free of charge to Defense contractors and to non-Defense agencies.

But the good news is that anyone can get the *Bulletin* one of two ways:

1. By accessing our DoDSI web page (http://www.dtic.mil/dodsi). We will send you an automatic e-mail notice via the Internet when a new issue goes on-line. Just enter your e-mail address on the registration form for this service in the *Security Awareness Bulletin* section of our web page.

2. By signing up for a low-cost subscription service that we have arranged through the U.S. Superintendent of Documents.

Here's how the Bulletin Subscription Service works: Send in a copy of the form below with a check for the appropriate amount and you will receive the *Bulletin* four times a year.

United States Government
INFORMATION

Order Processing Code
*5769

Credit card orders are welcome!

Fax your orders (202) 512-2250
Phone your orders (202) 512-1800

**Security Awareness Bulletin** at $9.00 ($11.25 foreign) per year
The total cost of my order is $ _____.

☐ YES, please send _____ subscription(s) to:

_____
Name or title (Please type or print)

_____
Company name Room, floor, suite

_____
Street address

_____
City State Zip +4

_____
Daytime phone including area code

_____
Purchase order number (optional)

For privacy protection, check the box below:

☐ Do not make my name available to other mailers

Check method of payment:

☐ Check payable to: Superintendent of Documents

☐ GPO Deposit Account ☐☐☐☐☐☐—☐

☐ Visa ☐ MasterCard

☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

(expiration date)

☐☐☐☐

_____
Authorizing signature

Mail to:
Superintendent of Documents, PO Box 371954, Pittsburgh PA 15250-7954

Important: Please include this completed order form with your remittance. *Thank you for your order!*

# Security Awareness Publications Available from the Institute

Publications are free. Just check the titles you want and send this form to us with your

address label

Our address is:

DoD Security Institute
Attn: Security Education & Awareness Team
8000 Jefferson Davis Hwy, Bldg 33E
Richmond, VA 23297-5091
(804) 279-4223 or DSN 695-4223;
FAX (804) 279-6406, DSN 695-6406

- ❑ **Recent Espionage Cases: Summaries and Sources**. May 1996. Eighty-eight cases, 1975 through 1995. "Thumb-nail" summaries and open-source citations.
- ❑ **Announcement of Products and Resources**. October 1996. A catalog of security education videos, publications, posters, and more you can order.
- ❑ **DELIVER!** Easy-to-follow pamphlet on how to transmit and transport your classified materials. Written specifically for the Department of Defense employee. February 1997.
- ❑ **Terminator VIII**. Requirements for destruction of classified materials. Written specifically for the Department of Defense employee. September 1992.
- ❑ **STU-III Handbook for Industry**. To assist FSOs of cleared defense contractors who require the STU-III, Type 1 unit. Covers step-by-step what you need to know and do to make the STU-III a valuable addition to your facility's operations.
- ❑ **Survival Handbook**. The basic security procedures necessary for keeping you out of trouble. Written specifically for the Department of Defense employee. March 1997.
- ❑ **Layman's Guide to Security**. The basic security procedures that you should be aware of when handling classified materials in your work environment. March 1997.
- ❑ **Acronyms and Abbreviations**. Twelve pages of security-related acronyms and abbreviations and basic security forms. October 1995.
- ❑ **Take A Security Break.** Questions and answers on security and other topics.
- ❑ **Take Another Security Break.** More questions and answers.
- ❑ **Lock Up!** A pamphlet on the structural standards and other security requirements for the storage of conventional arms, ammunition, and explosives. August 1995.

**Security Awareness Bulletin**. A quarterly publication of current security countermeasures and counterintelligence developments, training aids, and education articles. Back issues available from the Institute:

- ❑ The Case of Randy Miles Jeffries **(2-90)**
- ❑ Beyond Compliance - Achieving Excellence in Industrial Security **(3-90)**
- ❑ Foreign Intelligence Threat for the 1990s **(4-90)**
- ❑ Regional Cooperation for Security Education **(1-91)**
- ❑ AIS Security **(2-91)**
- ❑ Economic Espionage **(1-92)**
- ❑ What is the Threat and the New Strategy? **(4-92)**
- ❑ Acquisition Systems Protection **(1-93)**
- ❑ Treaty Inspections and Security **(2-93)**
- ❑ Research on Espionage **(1-94)**
- ❑ Acquisition Systems Protection Program **(3-94)**
- ❑ Aldrich H. Ames Espionage Case **(4-94)**
- ❑ Revised Self-Inspection Handbook/Summary of NISPOM Changes **(1-95)**
- ❑ The Threat to U.S. Technology **(2-95)**
- ❑ Entering a New Era in Security **(1-96)**
- ❑ Technical Security **(2-96)**
- ❑ Combating Terrorism **(3-96)**
- ❑ Profile of a Spy **(1-97)**
- ❑ Empowering the Security Professional **(2-97)**



*U.S. Government Printing Office: 1997 - 527-109/60003